

# نور در تاریکی

بخش 3 -



مؤسسة العزائم  
فارسی





در سال پنجم هجری، در ماه شوال، پیامبر محبوب ما محمد ﷺ جلسه‌ای با صحابه خود برگزار کرد، «چرا این جلسه برگزار شد؟»، دلیل این جلسه آن بود که قریش، با رهبری ابوسفیان، به همراه قبایل کنانه، بنی‌سلیم و دیگر قبایل، با نیرویی بالغ بر ده هزار نفر، قصد حمله و تصرف مدینه را داشتند.

در این جلسه، بحث اصلی بر سر دو راه‌برد نظامی بود: یا مانند جنگ بدر، در میدان باز به مقابله پرداختن، و یا همانند تجربه پس از نبرد احد، از درون شهر به دفاع برخاستن.

سلمان فارسی، که کنیه‌اش ابوعبدالله بود، در امپراتوری ساسانی به دنیا آمده و پیرو آیین زرتشتی بود، او بعدها به دین مسیحیت علاقه‌مند شد و سرانجام پس از دیدار با پیامبر اسلام ﷺ در مدینه، به اسلام گروید، با اشاره به تجربه‌اش در فارس، پیشنهاد داد که شهر مدینه با کندن خندق در اطراف آن مستحکم گردد، روشی نظامی که در امپراتوری ساسانی به کار گرفته می‌شد.

در نهایت، پیشنهاد او پذیرفته شد و مقرر گردید که هر ده نفر از مسلمانان، چهل ذراع از خندق را بکنند.

احتمالاً همه ما ادامه این داستان را می‌دانیم، در تاریخ، این نبرد به نام «غزه خندق» یا «غزه احزاب» معروف شد، در نتیجه پیروزی در این جنگ، اسلام بیش از پیش گسترش و نفوذ یافت.

# چرا پیامبر ﷺ پیشنهاد سلمان فارسی را پذیرفت، در حالی که این تاکتیک جنگی برای عرب‌ها ناآشنا بود؟

تا آن اندازه که به سطحی از تخصص برسیم و بهترین ابزار را کشف کنیم، این آگاهی، به ما قدرت می‌دهد که در زمان مناسب، ضربه‌ای قاطع بر دشمن وارد سازیم.

همزمان، باید اقدامات لازم را برای گریز از دام آنان نیز در نظر بگیریم، و این، هدف اصلی مجموعه‌ی «نور در تاریکی» است.

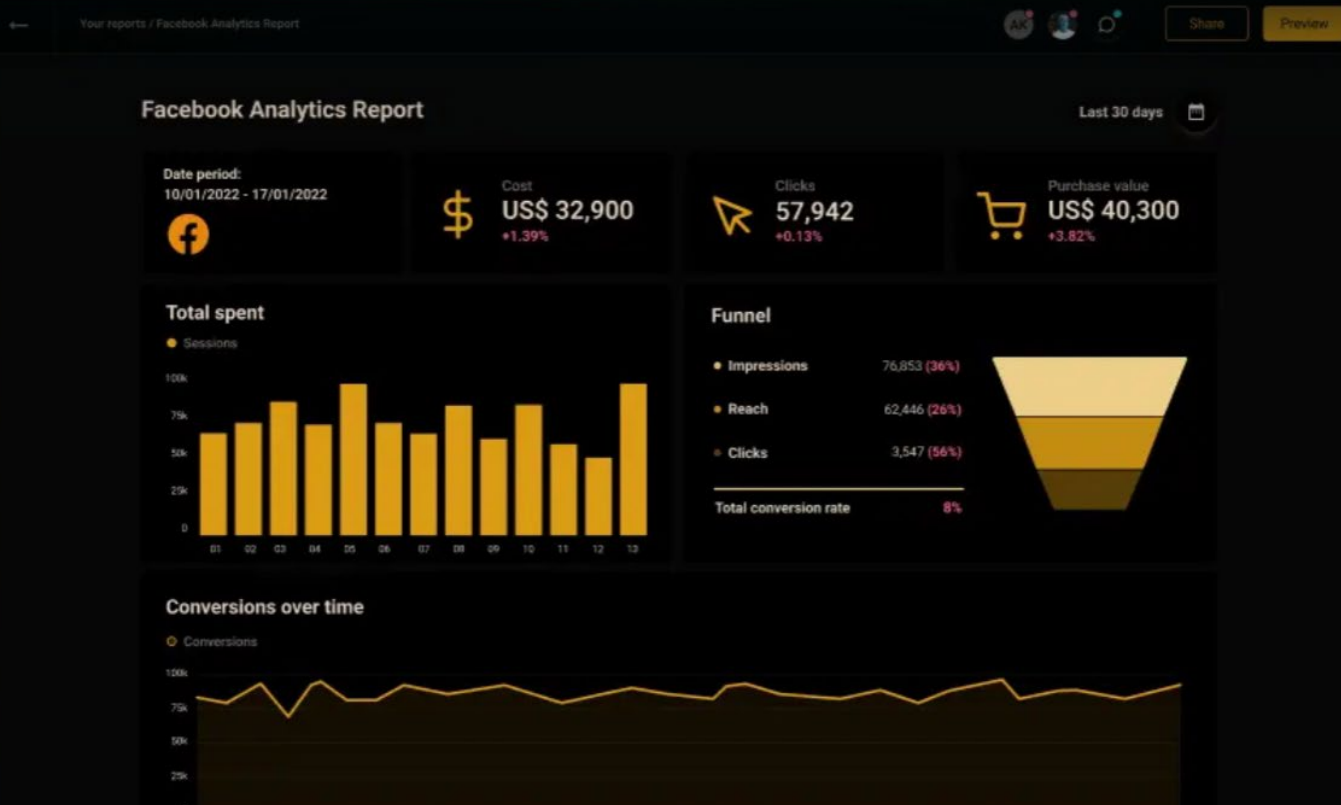
## «رسانه‌های اجتماعی چقدر امن هستند؟»

پاسخ این است: اینترنت به‌طور کامل امن نیست، و این موضوع به‌ویژه درباره برادران و خواهران موحد ما که با دشمنی جهانی مواجه‌اند، صدق می‌کند، بنابراین، این فضا نه‌تنها ناامن، بلکه می‌تواند خطری بزرگ برای آن‌ها باشد.

درسی که از این ماجرا می‌گیریم چنین است: «ما باید ابتدا تکنولوژی مناسب را بپذیریم، هرچند بهترین نباشد، فارغ از این‌که چه کسی آن را اختراع کرده یا در کجا پدید آمده است، و پس از آن، باید بر الله توکل کنیم.»

دقیقاً همین مسئله درباره تکنولوژی مدرن نیز صدق می‌کند، رسانه‌های اجتماعی همچون دام فناوری‌های هستند که کفار آن را برای به دام انداختن ما گسترانده‌اند، در عین حال، این رسانه‌ها بستری قوی برای ارتباط با برادران دینی‌مان و رساندن پیام‌مان به هر گوشه جهان در زمانی کوتاه را فراهم کرده‌اند.

باید از پیامبرمان ﷺ درس بگیریم، همچون او، باید شیوه‌ها و روش‌های دشمن را بیاموزیم،





همگی می‌دانیم که پلتفرم‌های رسانه اجتماعی، اغلب با رسوایی‌های مربوط به داده‌ها روبه‌رو هستند و به دولت‌ها کمک می‌کنند، این همکاری می‌تواند باعث شود افراد، برچسب «تندرو» بخورند، اگر به کمپین‌هایشان نگاهی بیندازید، متوجه می‌شوید که همیشه خود را آگاه نسبت به کلاهبرداری، هک، دزدی اطلاعات و دیگر تهدیدات نشان می‌دهند.

همه ما احتمالاً با تبلیغات در رسانه‌های اجتماعی آشنا هستیم، تبلیغات، منبع اصلی انتقام‌جویی فیسبوک است.

اما پرسش این است: این تبلیغات چگونه عمل می‌کنند؟

بیایید تبلیغات فیسبوک را با دقت بیشتری بررسی کنیم تا بفهمیم سازوکار آن‌ها چیست.

آیا توجه کرده‌اید که فید یا صفحه فیسبوک‌تان پر از تبلیغات شده است؟

نکته جالب اینجاست که تبلیغاتی که نمایش داده می‌شوند، برای هر کاربر منحصر به فرد هستند، گاهی می‌بینید که فید خبری شما پر شده از تبلیغاتی که واقعاً به آن‌ها نیاز دارید یا آن‌ها را می‌خواهید، این نتیجه یک الگوریتم پیشرفته و چشمگیر است که فیسبوک آن را توسعه داده است.

اما سؤال اینجاست: چطور فیسبوک از علاقه‌مندی‌ها و نیازهای من باخبر شده؟

آیا من مستقیماً این اطلاعات را در اختیار فیسبوک گذاشته‌ام؟

پاسخ، نگران‌کننده است، فیسبوک اطلاعات شما را می‌دزد - و همیشه چنین کرده است.

پس ای برادر و خواهر من، هنگام به اشتراک‌گذاری هرگونه اطلاعاتی در هر پلتفرم

رسانه اجتماعی، هوشیار باش.

برای درک بهتر این مسئله، چند نمونه واقعی از رسوایی‌های مربوط به داده‌ها را ذکر خواهم کرد که نشان می‌دهند چگونه داده‌های کاربران جمع‌آوری می‌شود.

کمبریج آنالیتیکا (Facebook):

در سال ۲۰۱۸، یک شرکت مشاوره سیاسی به نام کمبریج آنالیتیکا درگیر یک رسوایی بزرگ شد، ماجرا از یک اپلیکیشن تست شخصیت آغاز شد که توسط یک پژوهشگر ساخته شده بود، این اپلیکیشن توانست نه تنها داده‌های افرادی که آن را نصب کرده بودند، بلکه اطلاعات دوستان آن‌ها را نیز از فیسبوک جمع‌آوری کند، در نتیجه، اطلاعات شخصی میلیون‌ها کاربر فیسبوک بدون اطلاع‌شان به دست کمبریج آنالیتیکا افتاد.

گفته می‌شود این شرکت از این داده‌ها برای تلاش در جهت تأثیرگذاری بر رأی‌دهندگان در انتخابات ریاست جمهوری آمریکا در سال ۲۰۱۶ استفاده کرده است.

این نمونه‌ای آشکار است از این‌که چگونه رسانه‌های اجتماعی می‌توانند در خدمت دولت‌ها قرار گیرند.

بیایید نگاهی به دیگر رسوایی‌ها بیندازیم...



الگوریتم یوتیوب و ترویج اطلاعات نادرست:

الگوریتم پیشنهادی یوتیوب به دلیل ترویج محتوای جنجالی یا گمراه‌کننده - از جمله نظریه‌های توطئه - مورد انتقاد قرار گرفته است، این مسئله می‌تواند به گسترش اطلاعات غلط و اعتماد کاربران بر آن منجر شود.

دولت چین، نگرانی‌هایی وجود دارد، اینکه داده‌های جمع‌آوری شده توسط تیک‌تاک ممکن است برای نظارت یا مقاصد امنیتی به اشتراک گذاشته شوند.

در اینجا تنها چند مورد از رسوایی‌های بزرگ داده‌ای را ذکر کردیم، اما اگر در اینترنت جست‌وجو کنید، موارد بسیار بیشتری خواهید یافت، تمام این رسوایی‌ها به ما هشدار می‌دهند که هنگام استفاده از اینترنت باید هوشیار باشیم.

داده‌های ما در رسانه‌های اجتماعی چقدر ایمن‌اند؟

تا اینجا که این خط را می‌خوانید، حتماً بخش‌های قبلی را مطالعه کرده‌اید و می‌دانید چگونه شرکت‌های رسانه اجتماعی داده‌های شما را جمع‌آوری می‌کنند، واقعیت این است که داده‌های کاربران در رسانه‌های اجتماعی اساساً امن نیستند، و شما تنها با رعایت اصول امنیتی می‌توانید خطر را کاهش دهید.

اما برای برادران و خواهران مؤحد، این فضا کاملاً ناامن است؛ چرا که تمام شرکت‌های رسانه‌ای تحت نظارت دولت‌ها هستند، و بنابراین هرچه در این فضاها به اشتراک گذاشته شود، قابل ردیابی و پیگیری است، علاوه بر این، کلاهبرداری‌های داده‌ای بسیاری به‌طور مستمر در حال رخ دادن است.

بیایید چند نمونه را بررسی کنیم:

توییتر و کمپین‌های اطلاعات جعلی:

توییتر با مشکل جدی کمپین‌های انتشار اطلاعات نادرست مواجه شده است، در این کمپین‌ها، از حساب‌های جعلی و ربات‌ها برای پخش روایت‌های ساختگی و تأثیرگذاری بر افکار عمومی استفاده می‌شود، این نوع فعالیت‌ها گاهی با دخالت خارجی در مسائل اجتماعی مرتبط بوده‌اند.

اینستاگرام و نگرانی‌های مربوط به تصویر بدن: نگرانی‌ها درباره تأثیر منفی اینستاگرام بر سلامت روان و تصویر ذهنی نوجوانان در حال افزایش است، تمرکز این پلتفرم بر تصاویر آراسته و اغلب غیرواقعی، به دلیل ایجاد اضطراب و افسردگی مورد انتقاد قرار گرفته است، پژوهش‌ها نشان داده‌اند که این تأثیرات می‌تواند برای گروه‌های آسیب‌پذیر، به ویژه نوجوانان، بسیار مضر باشند.

نگرانی‌های مربوط به حریم خصوصی داده‌ها در تیک‌تاک:

درباره نحوه عملکرد تیک‌تاک در حوزه حفظ حریم خصوصی داده‌ها و احتمال ارتباطش با



## ۱ اپلیکیشن‌های جمع‌آوری داده:

کلاهبرداران اپ‌هایی یا برنامه‌های طراحی می‌کنند مانند بازی‌ها، نظرسنجی‌ها یا تست‌های شخصیتی که از شما اجازه دسترسی به داده‌های فیسبوکتان را می‌خواهند، در صورت دادن اجازه، این اپ‌ها اغلب بیش از حد لازم اطلاعات جمع‌آوری می‌کنند - حتی اطلاعات دوستانتان - که ممکن است بدون اطلاع شما فروخته یا سوءاستفاده شود.

## ۲ تبلیغات مخرب:

کلاهبرداران از پلتفرم تبلیغاتی فیسبوک برای انتشار آگهی‌هایی استفاده می‌کنند که شامل لینک‌هایی به وبسایت‌های آلوده یا بدافزار است. کلیک روی این لینک‌ها می‌تواند موجب جمع‌آوری داده‌های شما یا دسترسی به حساب فیسبوکتان شود.

## ۳ جعل هویت از طریق پروفایل‌های جعلی:

کلاهبرداران پروفایل‌هایی می‌سازند که وانمود می‌کنند دوست شما یا فردی مشهور هستند، آن‌ها ممکن است پیام‌هایی بفرستند که حاوی لینک یا درخواست اطلاعات حساس باشد.

## ۴ کلاهبرداری‌های تست و نظرسنجی:

برخی از تست‌ها و نظرسنجی‌های فیسبوک، اطلاعات شخصی گسترده‌ای از شما درخواست می‌کنند، در حالی‌که به ظاهر سرگرم‌کننده یا

آموزنده هستند، کلاهبرداران می‌توانند از این اطلاعات برای دزدی هویت یا فروش آن به طرف‌های دیگر استفاده کنند.

## ۵ حساب‌های کلون‌شده (شبیه سازی شده):

کلاهبرداران نسخه‌های جعلی از پروفایل‌های واقعی ایجاد می‌کنند و از تصاویر و اطلاعات در دسترس عمومی استفاده می‌نمایند، سپس به دوستان آن فرد پیام دوستی می‌فرستند تا به داده‌های شخصی‌شان دسترسی پیدا کنند.

## ۶ مهندسی اجتماعی:

در این روش، کلاهبرداران از اطلاعات شخصی جمع‌آوری‌شده از پروفایل فیسبوک استفاده می‌کنند تا کاربران را فریب دهند یا تحت تأثیر قرار دهند، ممکن است وانمود کنند دوست قابل اعتماد یا فردی آشنا هستند و از شما اطلاعات شخصی یا پول درخواست کنند.

علاوه بر این موارد مهم، تهدیدات دائمی مانند نشت داده‌ها وجود دارند، در گذشته، حجم زیادی از اطلاعات کاربران فیسبوک افشا شده است و ممکن است دوباره تکرار شود، هکرها می‌توانند از این داده‌ها برای حملات فیشینگ، سرقت هویت یا حتی تبلیغات هدفدار استفاده کنند، در حملات فیشینگ، کلاهبرداران پیام‌ها یا ایمیل‌های جعلی ایجاد می‌کنند که ظاهراً از سوی فیسبوک هستند، تا شما را به کلیک روی لینک یا افشای اطلاعات شخصی ترغیب کنند. «پس هوشیار و آگاه باشید تا قربانی این تهدیدها نشوید.»



چگونه می‌توانیم داده‌های خود را در رسانه‌های اجتماعی ایمن کنیم؟

برای محافظت از خود در برابر کلاهبرداری‌های رسانه اجتماعی، باید در اشتراک‌گذاری اطلاعات خود محتاط باشید، صحت حساب‌ها و وبسایت‌ها را قبل از تعامل با آن‌ها بررسی کنید، همیشه شکاک باشید و هرگونه پیشنهاد یا درخواست اطلاعات شخصی را دوباره چک کنید.

در حالی که داده‌های فیسبوک ۱۰۰ درصد امن نیستند، می‌توانید با انجام برخی اقدامات خود را تا حد ممکن از کلاهبرداری‌های داده‌ای در این پلتفرم محافظت کنید.

اما برای برادران و خواهران مؤحد، این فضا کاملاً ناامن است؛ چرا که تمام شرکت‌های رسانه‌ای تحت نظارت دولت‌ها هستند، و بنابراین هرچه در این فضاها به اشتراک گذاشته شود، قابل ردیابی و پیگیری است، علاوه بر این، کلاهبرداری‌های داده‌ای بسیاری به‌طور مستمر در حال رخ دادن است.

بیایید چند نمونه را بررسی کنیم:

## ۱ لینک‌ها را بررسی کنید:

قبل از کلیک بر روی هر لینکی، به ویژه در پیام‌ها، آدرس لینک را بررسی کرده و از لینک‌های مشکوک اجتناب کنید.

## ۲ پروفایل خود را خصوصی نگه دارید:

تنظیمات حریم خصوصی فیسبوک خود را طوری تنظیم کنید که فقط افرادی که می‌خواهید، اطلاعات شما را مشاهده کنند.

## ۳ استفاده از رمزهای عبور قوی و منحصر به فرد:

حساب خود را با یک رمز عبور قوی محافظت کنید و احراز هویت دو عاملی (2FA) را فعال کنید.

## ۴ استفاده از ویژگی‌های امنیتی:

با هوشیاری و استفاده از ویژگی‌های امنیتی موجود در فیسبوک، می‌توانید به حفاظت از داده‌های خود در برابر کلاهبرداری‌ها کمک کنید.

## ۵ حفاظت از پروفایل‌های اجتماعی:

برای محافظت از پروفایل‌های اجتماعی خود، استراتژی‌های مختلفی مانند استفاده از رمزهای عبور قوی و منحصر به فرد برای هر حساب اجتماعی وجود دارد، استفاده از یک مدیر رمز عبور (پسورد منیجر) برای پیگیری آن‌ها می‌تواند مفید باشد.

## ۶ فعال‌سازی احراز هویت دو مرحله‌ای (2FA):

این اقدام یک لایه امنیتی اضافی برای حساب شما ایجاد می‌کند.

## ۷ تنظیمات حریم خصوصی را تنظیم کنید:

تنظیمات حریم خصوصی خود را مرور کرده و تنظیمات لازم را انجام دهید تا بتوانید کنترل کنید که چه کسانی می‌توانند پست‌ها، اطلاعات پروفایل و فعالیت‌های شما را مشاهده کنند.



قبل از اشتراک‌گذاری هرگونه اطلاعات، دقت کنید:

در اشتراک‌گذاری اطلاعات آنلاین محتاط باشید. از قرار دادن اطلاعات حساس مانند آدرس خانه، شماره تلفن یا جزئیات مالی خودداری کنید.

مراقب تلاش‌های فیشینگ باشید:

در پیام‌ها یا لینک‌های ارسال شده از سوی کاربران ناشناس شک کنید، حتی اگر ظاهراً معتبر به نظر برسند.

استفاده از آخرین ویژگی‌ها:

همیشه از جدیدترین ویژگی‌ها و تنظیمات امنیتی پلتفرم‌های رسانه اجتماعی خود آگاه باشید و از آن‌ها استفاده کنید.

نظارت بر فعالیت‌های غیرعادی:

حساب خود را برای هرگونه دسترسی غیرمجاز یا فعالیت غیرعادی نظارت کرده و فوراً آن را گزارش دهید.

[برای رعایت بهترین شیوه‌ها، می‌توانید دو قسمت قبلی مجموعه «نور در تاریکی» را دنبال کنید.]

بیاپید این مقاله را با یادآوری یک رویداد مهم از تاریخ اسلام به پایان برسانیم.

در ماه ذوالقعدة، سال ۶ هجری، پس از دیدن این تاریخ، یک رویداد باید در ذهن همه ما باشد، در این روز، پیامبر عزیز ما ﷺ، بزرگ‌ترین انسان تاریخ، توافق‌نامه‌ای صلح میان مسلمانان و

قریش به نام «معاهده حدیبیه» را امضا کرد، در آن روز پیامبر ﷺ نه تنها معاهده‌ای امضا کرد بلکه راه را برای پیروزی مسلمانان هموار ساخت، این رویداد در سوره فتح به عنوان پیروزی آشکار از سوی الله تعالی اعلام شده است.

إِنَّا فَتَحْنَا لَكَ فَتْحًا مُبِينًا

«قطعاً ما برای تو پیروزی آشکاری آوردیم.» (فتح: ۱: ۴۸)

همه ما می‌دانیم که تصمیم‌گیری پیامبر ﷺ در آن زمان چقدر دشوار بود، اکثر صحابه، از جمله ابوبکر، علی و عمر رضی الله عنهم اجمعین، از این توافق‌نامه راضی نبودند، آن‌ها نمی‌خواستند بدون انجام عمره و حج به مدینه بازگردند، همچنین در ابتدا، برخی از شرایط معاهده به نظر می‌رسید که برخلاف منافع مسلمانان است، اما بعدها، آن‌ها تصمیم پیامبر ﷺ را درک کردند.

سؤال اینجاست: چرا پیامبر ما ﷺ با این پیمان موافقت کرد، در حالی که تمام صحابه آمادگی جنگ بودند؟ در قرآن کریم، الله متعال می‌فرماید:

﴿وَلَوْ قَاتَلَكُمُ الَّذِينَ يَن كَفَرُوا لَوْلَا الْأَدْبَرُ ثُمَّ لَا يُجِدُونَ وَلِيًّا وَلَا نَصِيرًا﴾

«و اگر کسانی که کفر ورزیدند با شما می‌جنگیدند، قطعاً پشت کرده می‌گریختند، و دیگر نه سرپرستی می‌یافتند و نه یاور.» (سوره فتح، آیه ۲۲)

در این آیه، الله تعالی وعده می‌دهد که اگر



مشرکان می‌جنگیدند، شکست می‌خوردند،  
اما با وجود این، پیامبر ﷺ پیمان صلح را  
پذیرفت.

اینجا پیامبر ﷺ درسی گران‌بها برای ما  
گذاشت: ما باید با حکمت با شرایط مواجه  
شویم، نه صرفاً با قدرت و هیجان.

وظیفه‌ی ما در این زمانه نیز چنین است،  
ما باید از تکنولوژی به‌درستی بهره ببریم و  
با احتیاط گام برداریم، باید دانش عمیق  
نسبت به تکنولوژی به‌دست آوریم و در این  
عرصه متخصص شویم، تا بتوانیم شبکه‌ی  
خود را تقویت کرده و در برابر هرگونه دشمنی  
مؤثرانه واکنش نشان دهیم، تا زمانی که به  
این توانمندی نرسیده‌ایم، باید از تکنولوژی  
های آنان استفاده کنیم، اما به شکلی امن و  
هوشیارانه.

